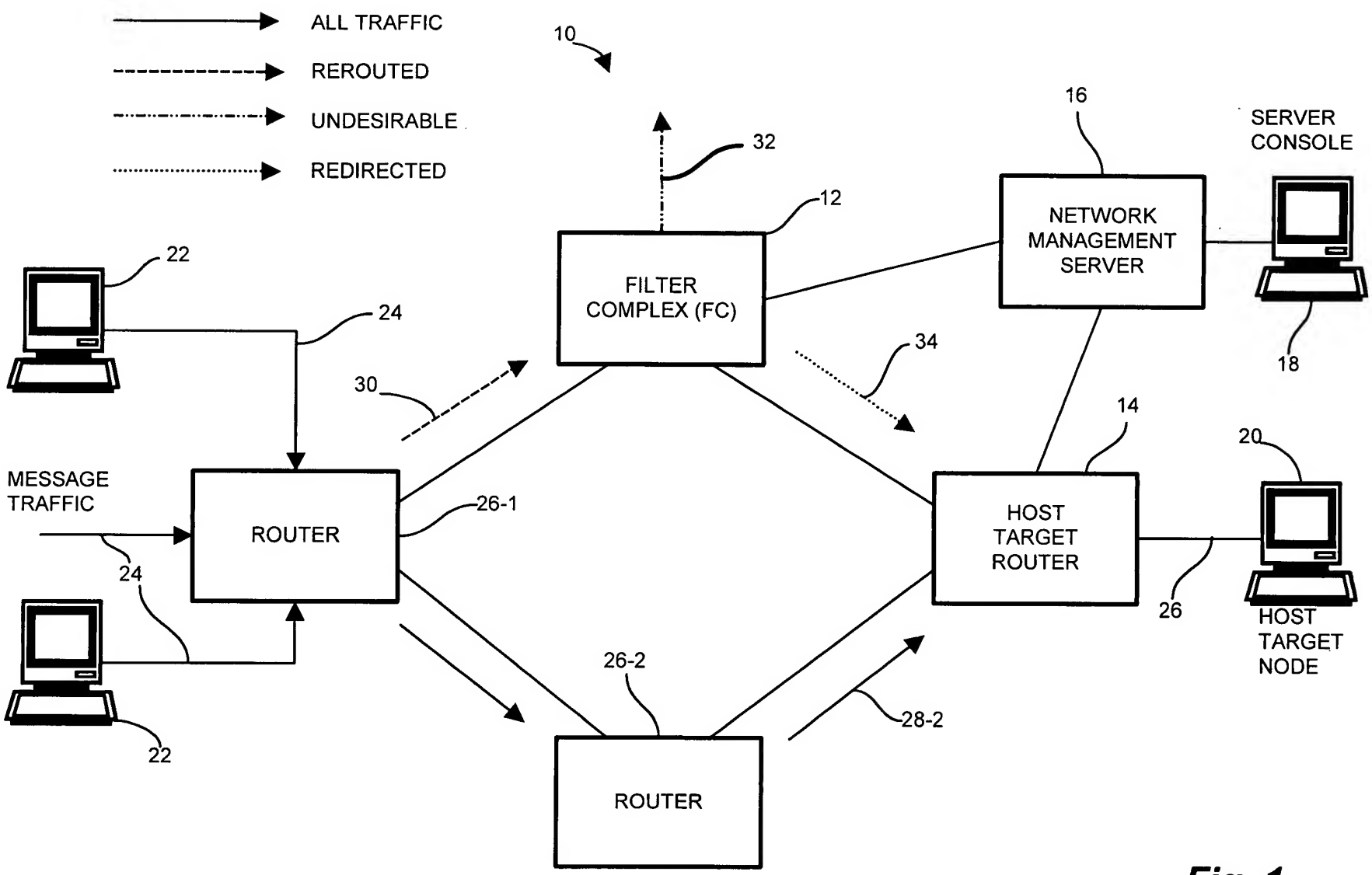
ALL TRAFFIC
REROUTED
UNDESIRABLE
REDIRECTED
10
32
12
16
SERVER CONSOLE
NETWORK MANAGEMENT SERVER
FILTER COMPLEX (FC)
22
24
30
34
18
14
20
MESSAGE TRAFFIC
ROUTER
26-1
HOST TARGET ROUTER
24
26
HOST TARGET NODE
22
26-2
28-2
ROUTER

Fig. 1

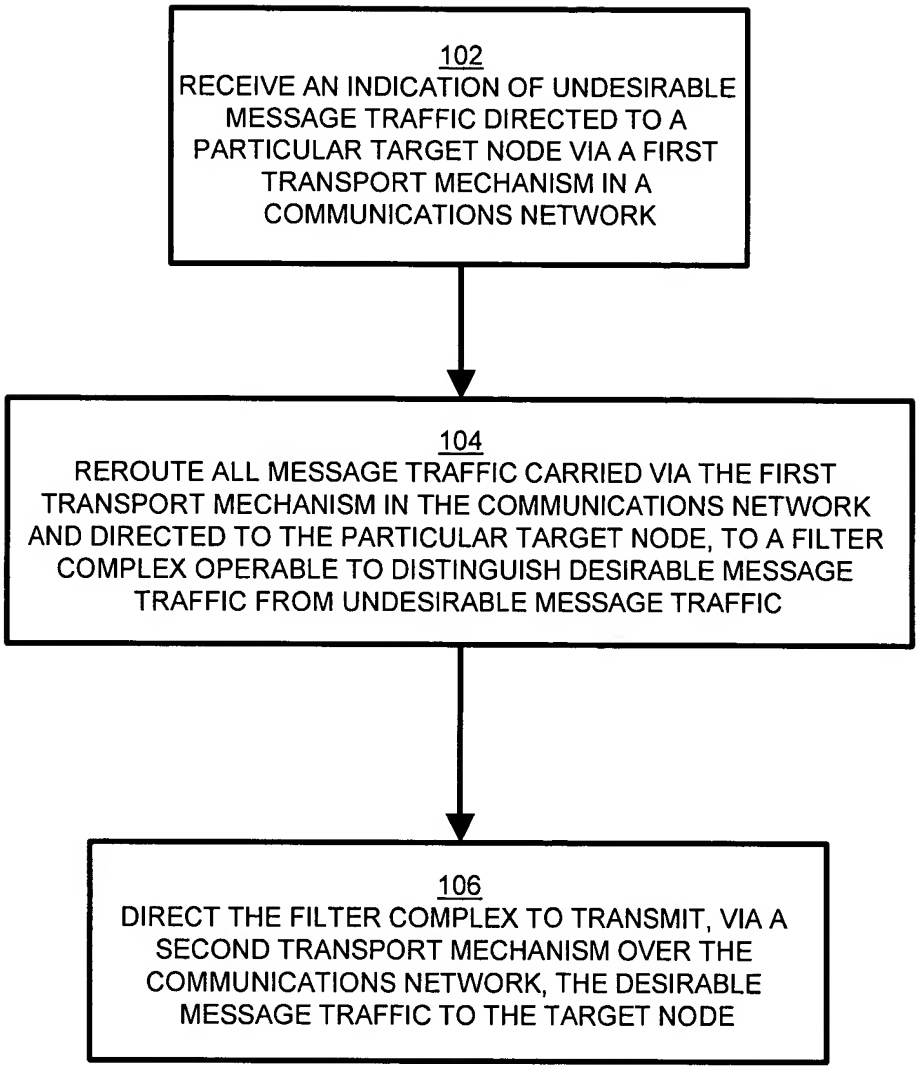
102
RECEIVE AN INDICATION OF UNDESIRABLE MESSAGE TRAFFIC DIRECTED TO A PARTICULAR TARGET NODE VIA A FIRST TRANSPORT MECHANISM IN A COMMUNICATIONS NETWORK
104
REROUTE ALL MESSAGE TRAFFIC CARRIED VIA THE FIRST TRANSPORT MECHANISM IN THE COMMUNICATIONS NETWORK AND DIRECTED TO THE PARTICULAR TARGET NODE, TO A FILTER COMPLEX OPERABLE TO DISTINGUISH DESIRABLE MESSAGE TRAFFIC FROM UNDESIRABLE MESSAGE TRAFFIC
106
DIRECT THE FILTER COMPLEX TO TRANSMIT, VIA A SECOND TRANSPORT MECHANISM OVER THE COMMUNICATIONS NETWORK, THE DESIRABLE MESSAGE TRAFFIC TO THE TARGET NODE

Fig. 2

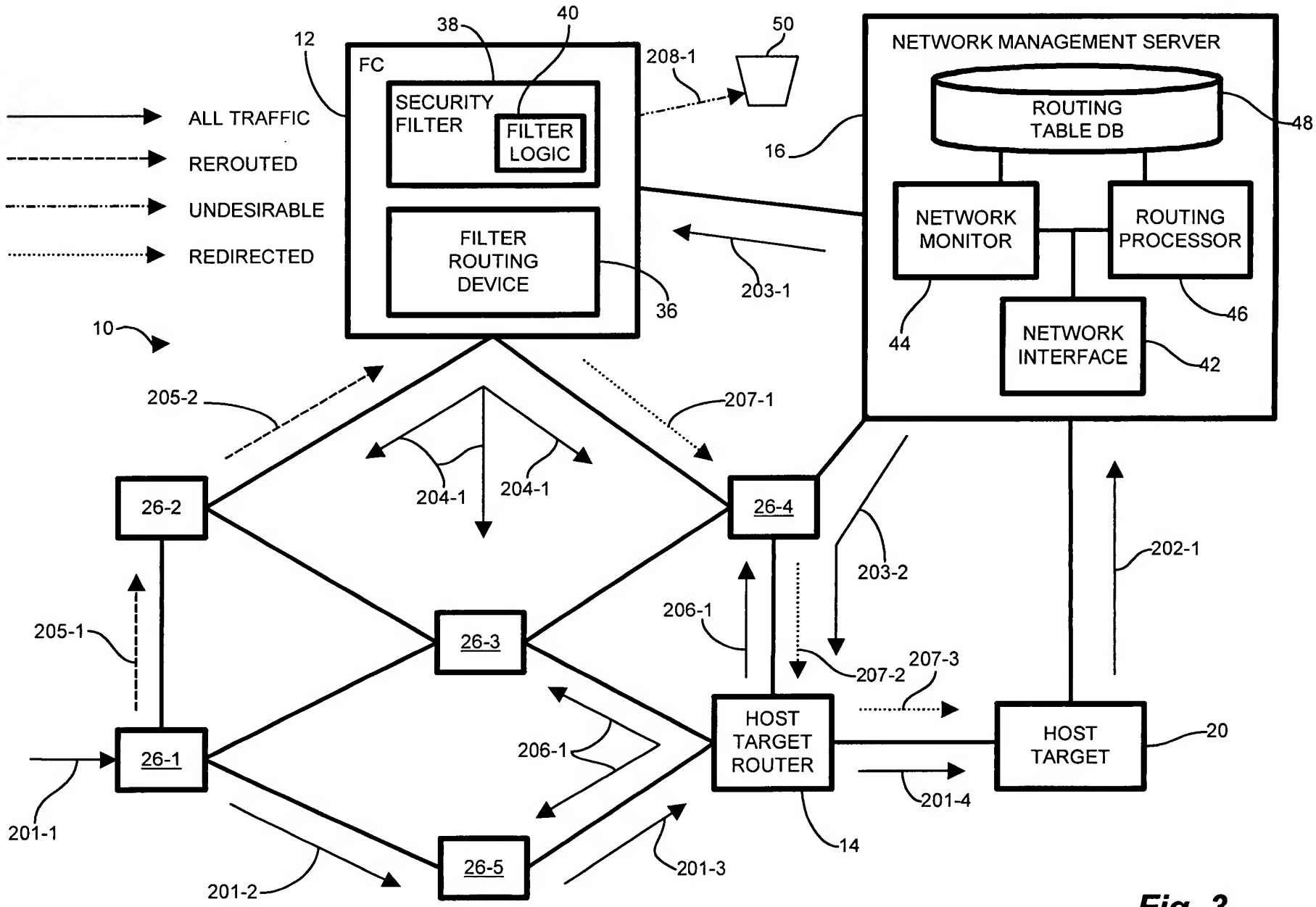
ALL TRAFFIC
REROUTED
UNDESIRABLE
REDIRECTED
12
FC
38
40
SECURITY FILTER
FILTER LOGIC
FILTER ROUTING DEVICE
36
208-1
50
16
NETWORK MANAGEMENT SERVER
ROUTING TABLE DB
48
NETWORK MONITOR
ROUTING PROCESSOR
46
44
NETWORK INTERFACE
42
203-1
10
205-2
207-1
204-1
204-1
26-2
26-4
26-3
205-1
206-1
203-2
202-1
207-2
207-3
HOST TARGET ROUTER
HOST TARGET
20
206-1
26-1
201-4
14
201-1
26-5
201-2
201-3

Fig. 3

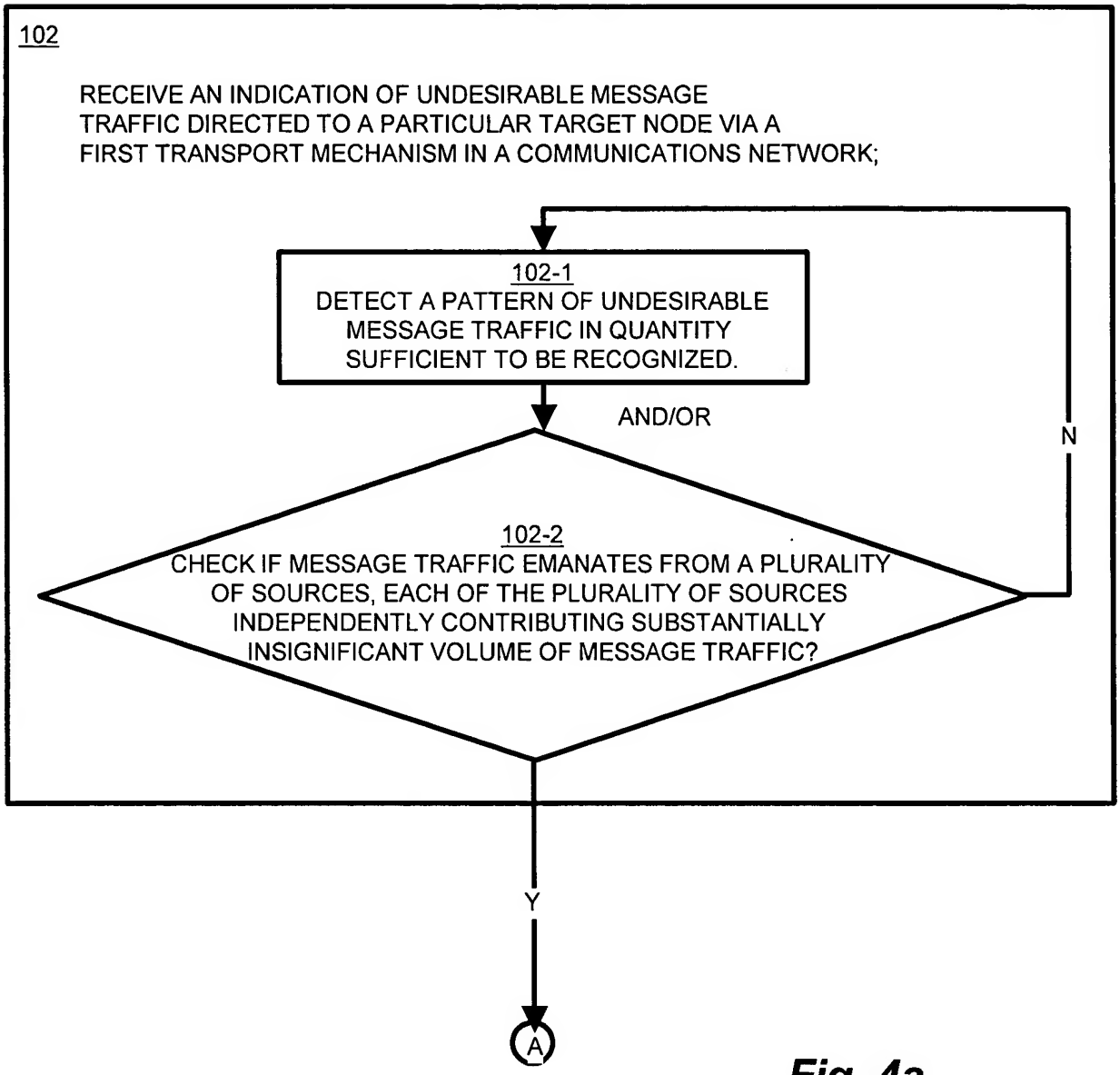
102
RECEIVE AN INDICATION OF UNDESIRABLE MESSAGE TRAFFIC DIRECTED TO A PARTICULAR TARGET NODE VIA A FIRST TRANSPORT MECHANISM IN A COMMUNICATIONS NETWORK;
102-1
DETECT A PATTERN OF UNDESIRABLE MESSAGE TRAFFIC IN QUANTITY SUFFICIENT TO BE RECOGNIZED.
AND/OR
102-2
CHECK IF MESSAGE TRAFFIC EMANATES FROM A PLURALITY OF SOURCES, EACH OF THE PLURALITY OF SOURCES INDEPENDENTLY CONTRIBUTING SUBSTANTIALLY INSIGNIFICANT VOLUME OF MESSAGE TRAFFIC?
N
Y
A

Fig. 4a

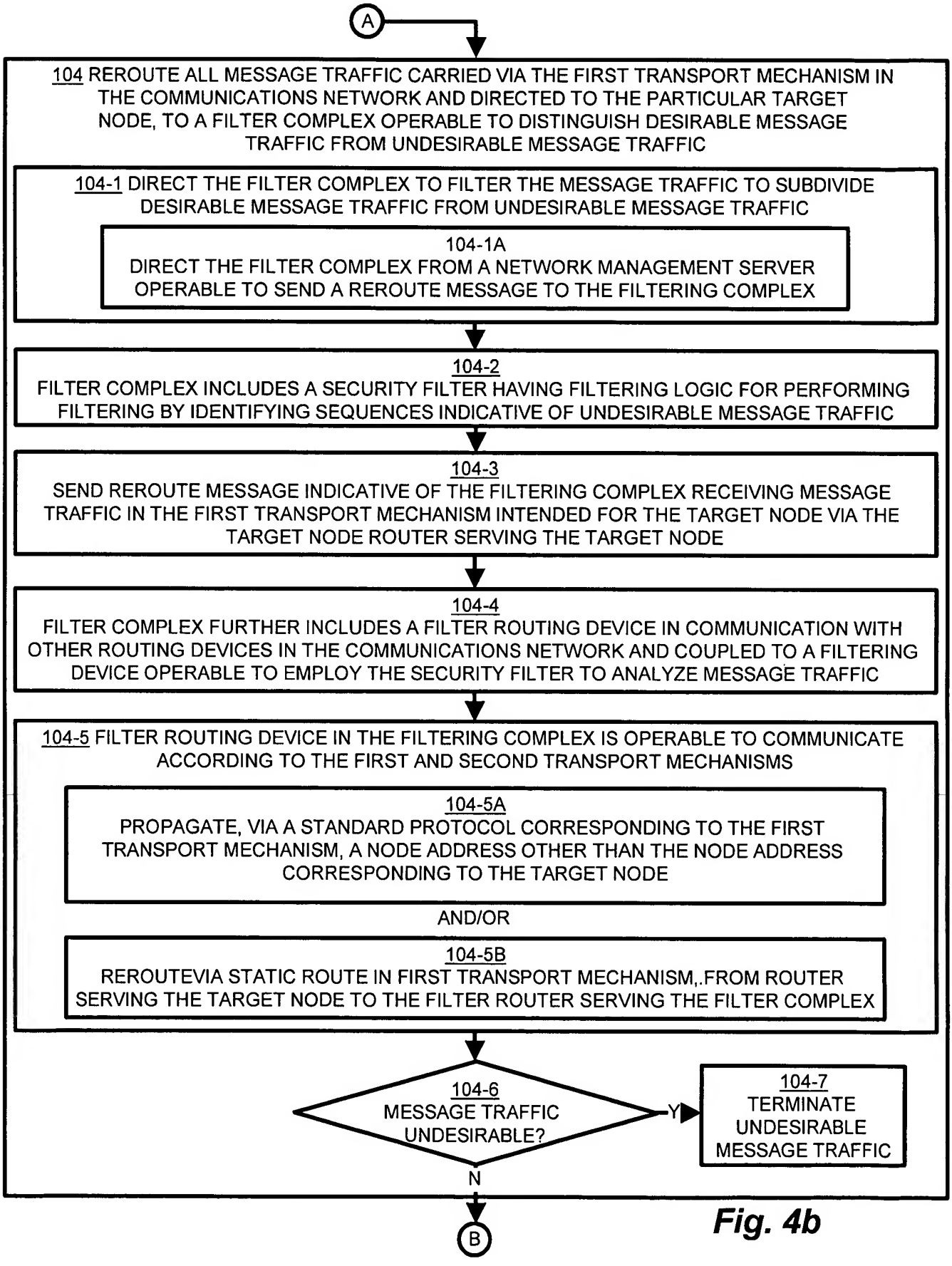
A
104 REROUTE ALL MESSAGE TRAFFIC CARRIED VIA THE FIRST TRANSPORT MECHANISM IN THE COMMUNICATIONS NETWORK AND DIRECTED TO THE PARTICULAR TARGET NODE, TO A FILTER COMPLEX OPERABLE TO DISTINGUISH DESIRABLE MESSAGE TRAFFIC FROM UNDESIRABLE MESSAGE TRAFFIC
104-1 DIRECT THE FILTER COMPLEX TO FILTER THE MESSAGE TRAFFIC TO SUBDIVIDE DESIRABLE MESSAGE TRAFFIC FROM UNDESIRABLE MESSAGE TRAFFIC
104-1A
DIRECT THE FILTER COMPLEX FROM A NETWORK MANAGEMENT SERVER OPERABLE TO SEND A REROUTE MESSAGE TO THE FILTERING COMPLEX
104-2
FILTER COMPLEX INCLUDES A SECURITY FILTER HAVING FILTERING LOGIC FOR PERFORMING FILTERING BY IDENTIFYING SEQUENCES INDICATIVE OF UNDESIRABLE MESSAGE TRAFFIC
104-3
SEND REROUTE MESSAGE INDICATIVE OF THE FILTERING COMPLEX RECEIVING MESSAGE TRAFFIC IN THE FIRST TRANSPORT MECHANISM INTENDED FOR THE TARGET NODE VIA THE TARGET NODE ROUTER SERVING THE TARGET NODE
104-4
FILTER COMPLEX FURTHER INCLUDES A FILTER ROUTING DEVICE IN COMMUNICATION WITH OTHER ROUTING DEVICES IN THE COMMUNICATIONS NETWORK AND COUPLED TO A FILTERING DEVICE OPERABLE TO EMPLOY THE SECURITY FILTER TO ANALYZE MESSAGE TRAFFIC
104-5 FILTER ROUTING DEVICE IN THE FILTERING COMPLEX IS OPERABLE TO COMMUNICATE ACCORDING TO THE FIRST AND SECOND TRANSPORT MECHANISMS
104-5A
PROPAGATE, VIA A STANDARD PROTOCOL CORRESPONDING TO THE FIRST TRANSPORT MECHANISM, A NODE ADDRESS OTHER THAN THE NODE ADDRESS CORRESPONDING TO THE TARGET NODE
AND/OR
104-5B
REROUTEVIA STATIC ROUTE IN FIRST TRANSPORT MECHANISM,.FROM ROUTER SERVING THE TARGET NODE TO THE FILTER ROUTER SERVING THE FILTER COMPLEX
104-6
MESSAGE TRAFFIC UNDESIRABLE?
Y
104-7
TERMINATE UNDESIRABLE MESSAGE TRAFFIC
N
B

Fig. 4b

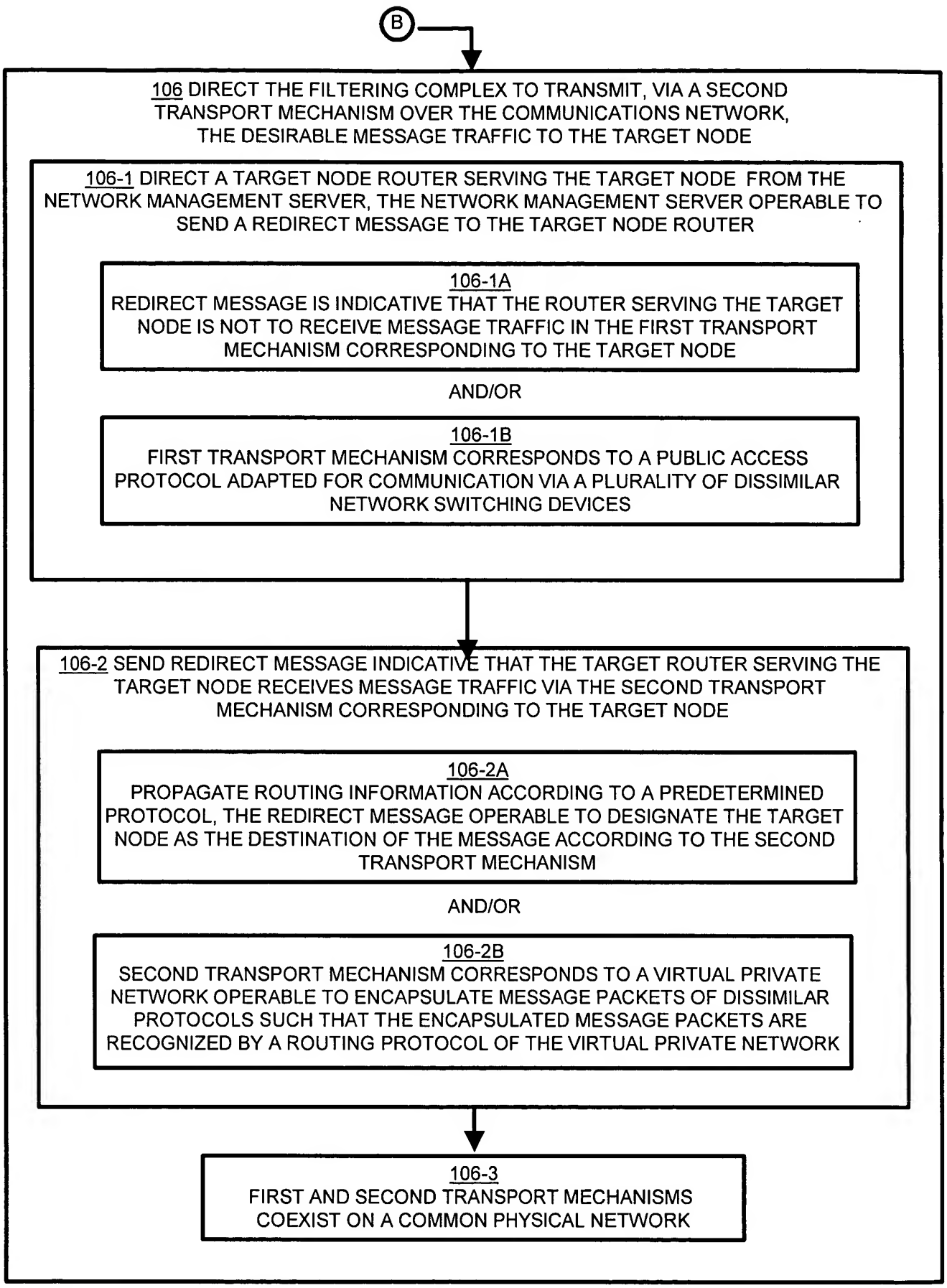
B
106 DIRECT THE FILTERING COMPLEX TO TRANSMIT, VIA A SECOND TRANSPORT MECHANISM OVER THE COMMUNICATIONS NETWORK, THE DESIRABLE MESSAGE TRAFFIC TO THE TARGET NODE
106-1 DIRECT A TARGET NODE ROUTER SERVING THE TARGET NODE FROM THE NETWORK MANAGEMENT SERVER, THE NETWORK MANAGEMENT SERVER OPERABLE TO SEND A REDIRECT MESSAGE TO THE TARGET NODE ROUTER
106-1A
REDIRECT MESSAGE IS INDICATIVE THAT THE ROUTER SERVING THE TARGET NODE IS NOT TO RECEIVE MESSAGE TRAFFIC IN THE FIRST TRANSPORT MECHANISM CORRESPONDING TO THE TARGET NODE
AND/OR
106-1B
FIRST TRANSPORT MECHANISM CORRESPONDS TO A PUBLIC ACCESS PROTOCOL ADAPTED FOR COMMUNICATION VIA A PLURALITY OF DISSIMILAR NETWORK SWITCHING DEVICES
106-2 SEND REDIRECT MESSAGE INDICATIVE THAT THE TARGET ROUTER SERVING THE TARGET NODE RECEIVES MESSAGE TRAFFIC VIA THE SECOND TRANSPORT MECHANISM CORRESPONDING TO THE TARGET NODE
106-2A
PROPAGATE ROUTING INFORMATION ACCORDING TO A PREDETERMINED PROTOCOL, THE REDIRECT MESSAGE OPERABLE TO DESIGNATE THE TARGET NODE AS THE DESTINATION OF THE MESSAGE ACCORDING TO THE SECOND TRANSPORT MECHANISM
AND/OR
106-2B
SECOND TRANSPORT MECHANISM CORRESPONDS TO A VIRTUAL PRIVATE NETWORK OPERABLE TO ENCAPSULATE MESSAGE PACKETS OF DISSIMILAR PROTOCOLS SUCH THAT THE ENCAPSULATED MESSAGE PACKETS ARE RECOGNIZED BY A ROUTING PROTOCOL OF THE VIRTUAL PRIVATE NETWORK
106-3
FIRST AND SECOND TRANSPORT MECHANISMS COEXIST ON A COMMON PHYSICAL NETWORK

Fig. 4c

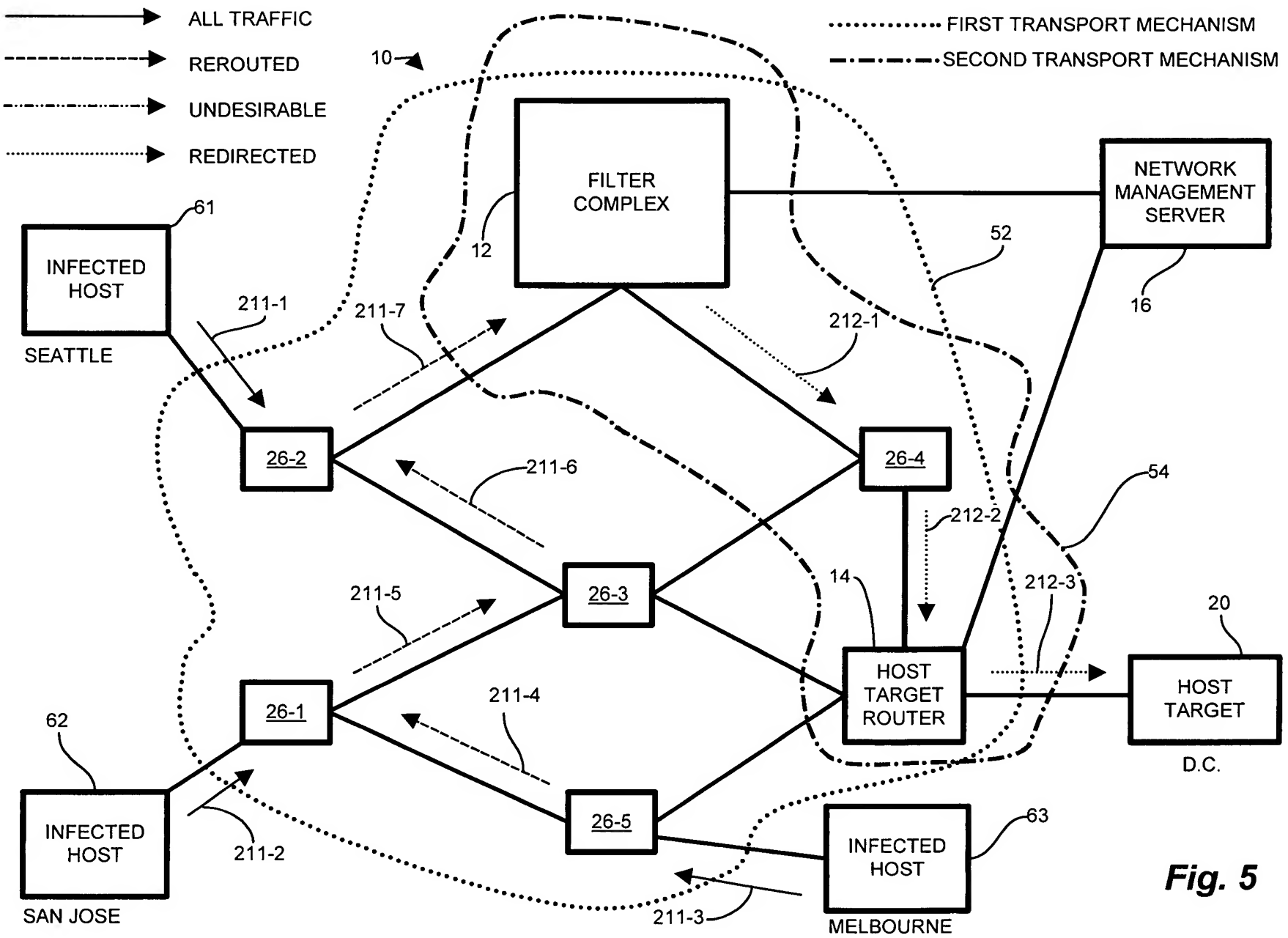
ALL TRAFFIC
REROUTED
UNDESIRABLE
REDIRECTED
FIRST TRANSPORT MECHANISM
SECOND TRANSPORT MECHANISM
10
FILTER COMPLEX
12
NETWORK MANAGEMENT SERVER
16
52
INFECTED HOST
61
SEATTLE
211-1
211-7
212-1
26-2
26-4
211-6
54
212-2
14
26-3
211-5
212-3
20
HOST TARGET ROUTER
HOST TARGET
D.C.
26-1
211-4
62
INFECTED HOST
SAN JOSE
211-2
26-5
INFECTED HOST
63
MELBOURNE
211-3

Fig. 5